<u>REMARKS/ARGUMENTS</u>

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3-5, 7-9 and 11-18 are pending in the application. Claims 1, 7, 9, 11 and 13 are amended; and Claims 6 and 10 are canceled without prejudice or disclaimer by the present amendment. Support for the amended claims can be found in the original specification, claims and drawings.[1] No new matter is presented.

In the Office Action, Claims 1 and 3-12 are rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. 6,248,946 to <u>Dwek</u> in view of U.S. Pub. 2002/0032027 to <u>Kirani</u>.

In response to this rejection, Applicant respectfully submits that amended independent Claims 1, 9 and 13 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1, for example, recites, in part, a user authentication method for an authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

> registering, at an authentication server, unique identification information corresponding to a mobile information terminal, *the unique information including a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal* ...
> receiving, at the authentication server from said mobile information terminal, the unique identification information *as encrypted by a predetermined encryption algorithm by a Web browser installed on said mobile information terminal*, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via a network ...

---

[1] e.g., specification, at least at Figs. 5-7 and p. 18, l. 2 – p. 10, l. 15.

Independent Claims 9 and 13, while directed to alternative embodiments, are amended to recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of amended independent Claims 1, 9 and 13.

In rejecting the claimed features directed to registering unique identification information corresponding to an information terminal, the Office Action relies on col. 4, ll. 31-43 of Dwek. This cited portion of Dwek describes a client interface server 112 that provides an Internet home page through which a new user may establish a connection with the online music delivery system 100. Dwek describes that a new user may register with the online music service and download an installation file for installing a copy of the music player 120 onto the user's computer.

Thus, Dwek does appear to describe that the a new user may register with the online music service, but fails to teach or suggest "registering, at an authentication server, unique identification information corresponding to a mobile information terminal, *the unique information including a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal*" as recited in amended independent Claim 1.

Further, in rejecting the claimed features directed to receiving the unique identification information at the authentication server from the mobile information terminal, the Office Action relies on col. 9. ll. 31-45, and col. 10, ll. 21-47 and 60-67 of Dwek. This cited portion of Dwek describes the ability for a user to create and share a "user defined channel". This process includes setting up a play list, which is stored at the online music library, and allowing the music in the play list to be streamed to a user's computer.

This cited portion of Dwek, however, fails to teach or suggest "receiving, at the authentication server from said mobile information terminal, the [registered] unique identification information [including a manufacturer code identifying the manufacturer of the

9

mobile information terminal and an identification code unique to the mobile information

terminal] *as encrypted by a predetermined encryption algorithm by a Web browser installed*

on said mobile information terminal ..." as recited in amended independent Claim 1.

In rejecting a similar features recited in previously pending dependent Claim 6, the

Office Action relies on col. 5, ll. 31-43 of Dwek and paragraph [0222] of Kirani.

Col. 5, ll. 31-43 of Dwek describes an audio interface 240 that interfaces the

decompressed song file from a decompressor 230 to audio processing components of a

personal computer. As an initial matter, this process involves decompressing a song file

received at the personal computer from the online music service, and is not related to

"receiving, at the authentication server from said mobile information terminal, the unique

identification information ..." as recited in Claim 1. Moreover, the process of decompressing

a song received at a personal computer is in no way analogous to "receiving, at the

authentication server from said mobile information terminal, the [registered] unique

identification information [including a manufacturer code identifying the manufacturer of the

mobile information terminal and an identification code unique to the mobile information

terminal] *as encrypted by a predetermined encryption algorithm by a Web browser installed*

on said mobile information terminal ..." as recited in amended independent Claim 1.

Further, paragraph [0222] of Kirani describes a process of generating a globally

unique picture ID (GUID) for each picture taken, which is represented by an ASCII character

string. Thus, this cited portion of Kirani does not appear to be related to transmitting unique

identification information, whatsoever, much less encrypting and transmitting said unique

identification.

Therefore, Dwek, even if combined with Kirani, fails to teach or suggest a user

authentication method for an authentication server which executes user authentication

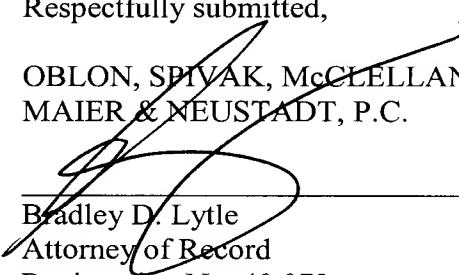between a mobile information terminal and a content providing server interconnected by an

open network, the method comprising "registering, at an authentication server, unique

identification information corresponding to a mobile information terminal, *the unique*

information including a manufacturer code identifying the manufacturer of the mobile

information terminal and an identification code unique to the mobile information terminal

... [and] receiving, at the authentication server from said mobile information terminal, *the*

[registered] unique identification information [including a manufacturer code identifying the

manufacturer of the mobile information terminal and an identification code unique to the

mobile information terminal] *as encrypted by a predetermined encryption algorithm by a*

Web browser installed on said mobile information terminal, and a request for registering

one of said official site access information for accessing said content providing server with a

personal menu via a network ..." as recited in amended independent Claim 1.

Accordingly, Applicant respectfully requests that the rejection of Claims 1, 3-5, 7-9

and 11-18 under 35 U.S.C. § 103 be withdrawn.

Consequently, in view of the present amendment and in light of the foregoing

comments, it is respectfully submitted that the invention defined by Claims 1, 3-5, 7-9 and

11-18 is patentably distinguishing over the applied references. The present application is

therefore believed to be in condition for formal allowance and an early and favorable

reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Andrew T. Harry
Registration No. 56,959

I:\ATTY\ATH\PROSECUTION\21S\212668-US\212668US - AM DUE 01-09-09.DOC